

**ÜBER EINBETTUNGSEIGENSCHAFTEN
VON NORMALTEILERN, DIE DER HYPERZENTRALEN
EINBETTUNG ÄHNLICH SIND**

von

Wolfdieter Nowak

aus

Rumburg

1972

**ÜBER EINBETTUNGSEIGENSCHAFTEN
VON NORMALTEILERN, DIE DER HYPERZENTRALEN
EINBETTUNG ÄHNLICH SIND**

Der Naturwissenschaftlichen Fakultät
der Friedrich-Alexander-Universität Erlangen-Nürnberg
zur
Erlangung des Doktorgrades

vorgelegt

von

Wolfdieter Nowak

aus

Rumburg

Als Dissertation genehmigt von der
Naturwissenschaftlichen Fakultät
der Universität Erlangen-Nürnberg



Tag der mündlichen Prüfung: 29. November 1972

Dekan:	Prof. Dr. W. Heumann
Erstberichterstatter:	Prof. Dr. H. Heineken
Zweitberichterstatter:	Prof. Dr. W. Specht

Inhalt

	Vorwort	1
	Verzeichnis der Symbole	3
1.	Vorbemerkungen	5
2.	Einbettungsgesetze bezüglich eines abelschen Normalteilers	10
3.	Einbettungsgesetze mit Kommutator- eigenschaften	33
	Literaturverzeichnis	42



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548612_0044

Vorwort:

Der Beweis eines Satzes von P. Hall [1, Theorem 7] beruht im wesentlichen auf folgendem Lemma [1, Lemma 7], das in Kommutatorschreibweise lautet:

Wenn in einer Gruppe G für einen Normalteiler N und eine natürliche Zahl i

$$\underbrace{[\dots [[N, G], G], \dots, G]}_{i\text{-mal}} \leq N_2$$

ist, dann ist für jede natürliche Zahl r

$$\underbrace{[\dots [[N_r, G], G], \dots, G]}_{r(i-1)+1\text{-mal}} \leq N_{r+1}.$$

Diese Aussage soll in dem Sinn verallgemeinert werden, daß der Kommutator $[N, G]$ durch ein Wort $w(N, G)$ und iterierte Kommutatoren $\underbrace{[\dots [[N, G], G], \dots, G]}_{j\text{-mal}}, j \in \mathbb{N}$, durch iterierte Wörter

$w^j(N, G^j)$ ersetzt werden.

Gefragt ist nach der Gestalt der Wörter $w(N, G)$ für welche diese neue Aussage wahr ist.

Um diese Wörter zu charakterisieren, werden zwei Fragen angegangen:

1. Wie kann man die Einbettungsgesetze in einer Variablen bezüglich eines abelschen Normalteilers klassifizieren?

Diese Frage behandelt Abschnitt 2. Es stellt sich dabei heraus, daß die Situation wesentlich einfacher ist, wenn man zusätzlich einen Primzahlexponenten für den Normalteiler vorschreibt.

2. Welche Einbettungsgesetze w sind so beschaffen, daß für je zwei Normalteiler M und N von G gilt:

$$w([N, M], G) \leq [w(N, G), M] [N, w(M, G)] [N, M, M] [N, M, N] \quad ?$$

Diese Frage behandelt Abschnitt 3. Die Beziehung wird zum Beispiel von

$$w(N, G) = [N, G]$$

erfüllt (vergl. [1, Lemma 1]).

Diese Fragen werden übertragen auf das Problem, gewisse Ideale in den Gruppenringen $\mathbb{Z}\langle x \rangle$ bzw. $\mathbb{Z}\langle x_1, x_2 \rangle$ zu charakterisieren. Die Übertragung beruht auf der Tatsache, daß sich jedes Wort $w(y, x)$ mit der Eigenschaft

$$\bigwedge_{y \in N} \bigwedge_{x \in G} w(y, x) \in N_2$$

als Produkt von Konjugierten von y schreiben läßt. Der durch diese Konjugationen gegebene Endomorphismus von N/N_2 kann durch ein Element $F(x)$ aus $\mathbb{Z}\langle x \rangle$ beschrieben werden. Die Charakterisierung der Wörter $w(y, x)$ erfolgt dann durch die Bestimmung geeigneter Ideale in den erwähnten Gruppenringen.

An dieser Stelle möchte ich Herrn Professor Dr. H. Heineken für die Überlassung des Themas und die vielen Anregungen und Ratschläge danken, die mir die Fertigstellung dieser Arbeit ermöglichten.

Verzeichnis der Symbole:

$\mathbb{N}$	Menge der natürlichen Zahlen
$\mathbb{Z}$	Menge oder Ring der ganzen Zahlen
$\mathbb{Q}$	Menge oder Körper der rationalen Zahlen
$\mathbb{Z}_{p^n}$	Restklassenring der ganzen Zahlen mod p^n (p Primzahl, $n \in \mathbb{N}$)
$R[x], R[x_1, x_2]$	Polynomring in einer bzw. zwei Variablen über dem Ring R
$R\langle x \rangle, R\langle x_1, x_2 \rangle$	Gruppenring, gebildet aus dem Ring R und der freien abelschen Gruppe vom Rang 1 bzw. 2
$\bar{\sigma}_n(x)$	n -tes Kreisteilungspolynom
$[x, y] := x^{-1}y^{-1}xy$	
$x^y := y^{-1}xy$	
$N \leq G$	N ist Untergruppe bzw. Unterring der Gruppe bzw. des Rings G .
$N \trianglelefteq G$	N ist Normalteiler bzw. Ideal der Gruppe bzw. des Rings G .
G/N	Faktorgruppe bzw. Faktorring von G nach N
$U \cong V$	Isomorphie zwischen Gruppen oder Ringen
$\langle K \rangle$	die von dem Komplex K erzeugte Gruppe (Ring)
$\langle K \rangle^G$	normaler Abschluß des Komplexes K in der Gruppe G
$[U, V] = \langle \{x \mid x = [u, v], u \in U, v \in V\} \rangle$	für Untergruppen U und V einer Gruppe G
$[U, V, W] := [[U, V], W]$	
$N_{k+1} := [N_k, N]; N_1 := N$	
$w(x, y)$	Wort, d.h. Element der von x und y erzeugten freien Gruppe
$w(N, G)$	Wortuntergruppe von G mit Elementen $x \in N$ und $y \in G$

$$w^{k+1}(N, G^{k+1}): = w(w^k(N, G^k), G); w^0(N, G): = N$$

$r|s$ In einem Ring R existiert zu $r \in R$ und $s \in R$
ein Element $t \in R$ mit $t \cdot r = s$.

// Ende eines Beweises

1. Vorbemerkungen

Wir gehen aus von der Aussage ([1, Lemma 7]):

(A) Wenn in einer Gruppe G für einen Normalteiler N und eine natürliche Zahl i

$$N/N_2 \leq Z_i(G/N_2)$$

ist, dann ist für jede natürliche Zahl r

$$N_r/N_{r+1} \leq Z_{r(i-1)+1}(G/N_{r+1}).$$

Ziel der vorliegenden Arbeit ist es, die Wörter $w(y,x), y \in N, x \in G$, anzugeben, für welche die entsprechende Aussage richtig bleibt. Das heißt, es soll folgendes Problem behandelt werden:

(B) Für welche Wörter $w(y,x)$ gilt die Aussage:

Wenn in einer Gruppe G für einen Normalteiler N und eine natürliche Zahl i

$$w^i(N, G) \leq N_2$$

ist, dann ist für jede natürliche Zahl r

$$w^{r(i-1)+1}(N_r, G^{r(i-1)+1}) \leq N_{r+1}.$$

Die Aussage (A) liefert, daß $w(y,x) = [y,x]$ zu den gesuchten Wörtern gehört. Denn bekanntlich ist

$$N/N_2 \leq Z_i(G/N_2)$$

gleichwertig mit

$$\left[\dots \underbrace{\left[\left[N, G \right], G \right], \dots, G}_{i\text{-mal}} \right] \leq N_2.$$

In diesem Sinn ist also die Aussage (A) als Spezialfall in (B) enthalten.

Bei der Charakterisierung der Wörter $w(y, x)$ wird man deshalb den Beweis der Aussage (A) zu analysieren versuchen. Eine gewisse Vorauswahl kann bei der Behandlung des Problems (B) durch die Untersuchung der folgenden Frage getroffen werden:

(C) Welche Darstellung lassen die Wörter $w(y, x)$ zu, für die gilt:

$$(I) \quad \bigwedge_{y \in N} \bigwedge_{x \in G} w(y, x) \in N_2$$

Diese Untersuchung erleichtert die Handhabung des Problems:

(D) Aus den die Bedingung (I) erfüllenden Wörtern $w(y, x)$ suche man alle diejenigen, die die Bedingung erfüllen:

(II) Für je zwei Normalteiler U und V der Gruppe G gilt

$$w([U, V], G) \leq [w(U, G), V] [U, w(V, G)] [U, V, V] [U, V, U] .$$

Diese Bedingung kann man als die Übertragung der Aussage des "Drei-Untergruppen-Lemmas" von P. Hall [1, Lemma 1] auf unser Problem auffassen. Dieses Lemma liefert die Grundlage für den Beweis der Aussage (A). Es zeigt sich, daß die aus (C) und (D) sich ergebenden Wörter $w(y, x)$ zu den in Problem (B) angesprochenen gehören.

Zur Vorbereitung dienen die beiden folgenden Hilfssätze:

Hilfssatz 1: Wenn in einer Gruppe G mit den Normalteilern U und V ein Wort w die Bedingung (I) erfüllt, dann ist

$$w(UV, G) \leq w(U, G)w(V, G) \mod [U, V].$$

Beweis: Jedes Wort $w(y, x)$ läßt sich schreiben als ein Produkt

$$w(y, x) = x^r \prod_i y^{s_i}$$

mit gewissen Exponenten r und s_i . Falls $r \neq 0$ ist, wählen wir statt $w(y, x)$ das neue Wort $w'(y, x) = w(e, x)^{-1} w(y, x)$, das die Bedingung (I) ebenfalls erfüllt. Wir können uns daher auf den Fall $r=0$ beschränken und $w(y, x)$ als Produkt von Konjugierten von y schreiben.

$$\begin{aligned} \bigwedge_{u \in U} \bigwedge_{v \in V} \bigwedge_{x \in G} w(uv, x) &= \prod_i (uv)^{x^{s_i}} = \\ &= \prod_i u^{x^{s_i}} \prod_i v^{x^{s_i}} \mod [U, V] = \\ &= w(u, x)w(v, x) \mod [U, V], \end{aligned}$$

mit geeigneten ganzen Zahlen s_i .

//

Hilfssatz 2: Wenn in einer Gruppe G mit den Normalteilern U und V ein Wort w die Bedingungen (I) und (II) erfüllt, dann ist

$$\begin{aligned} \bigwedge_{i \in \mathbb{N}} w^i([U, V], G^i) &= \prod_{m+n=i} [w^m(U, G^m), w^n(V, G^n)] \\ &\mod [U, V, V][U, V, U]. \end{aligned}$$

Beweis: Für $i=1$ ist diese Aussage wahr.

Angenommen, sie ist auch wahr für ein $i \geq 1$. Dann gilt:

$$w^{i+1}([U, V], G^{i+1}) = w(w^i([U, V], G^i), G) \leq$$

$$\begin{aligned}
 &\leq w\left(\prod_{m+n=i} [w^m(U, G^m), w^n(V, G^n)], G\right) \mod [U, V, V] [U, V, U] \\
 &\quad (\text{nach Hilfssatz 1}) \\
 &\leq \prod_{m+n=i} w\left([w^m(U, G^m), w^n(V, G^n)], G\right) \mod [U, V, V] [U, V, U] \\
 &\leq \prod_{m+n=i} [w^{m+1}(U, G^{m+1}), w^n(V, G^n)] [w^m(U, G^m), w^{n+1}(V, G^{n+1})] \\
 &\quad \mod [U, V, V] [U, V, U] \\
 &\leq \prod_{m+n=i+1} [w^m(U, G^m), w^n(V, G^n)] \mod [U, V, V] [U, V, U] \\
 &\quad //
 \end{aligned}$$

Satz 1: Jedes Wort w , das die Bedingungen (I) und (II) erfüllt, gehört zu der in Problem (B) angegebenen Menge.

Beweis: Für $r=1$ erhält man die Voraussetzung.

Angenommen, der Satz ist richtig für $r \geq 1$. Dann gilt:

$$\begin{aligned}
 &w^{(r+1)(i-1)+1}(N_{r+1}, G^{(r+1)(i-1)+1}) = \\
 &= w^{(r+1)(i-1)+1}([N_r, N], G^{(r+1)(i-1)+1}) \leq \\
 &\leq \prod_{\substack{m+n= \\ (r+1)(i-1)+1}} [w^m(N_r, G^m), w^n(N, G^n)] \mod N_{r+2} \\
 &\leq [N_{r+1}, N] [N_r, N_2] \leq N_{r+2}
 \end{aligned}$$

Die vorletzte Ungleichung gilt, da für $n < i$ nach Induktionsannahme

$$w^m(N_r, G^m) \leq N_{r+1}$$

und in allen anderen Fällen

$$w^m(N_r, G^m) \leq N_r \quad \text{und} \quad w^n(N, G^n) \leq N_2$$

ist.

//

Bemerkung: Wir werden später zeigen, daß auch die Umkehrung gilt (Satz 8).

2. Einbettungsgesetze bezüglich eines abelschen Normalteilers

In der Bedingung (I) für die Wörter w wird gefragt, auf welchen Typ man sich beschränken kann, wenn die Wörter die Eigenschaft

$$\bigwedge_{y \in N} \bigwedge_{x \in G} w(y, x) \in N_2$$

haben sollen.

Hat ein Wort diese Eigenschaft, kann es ö.B.d.A. als Produkt von Konjugierten von y geschrieben werden

$$(*) \quad w(y, x) = \prod_i y^{x^{s_i}},$$

mit gewissen Zahlen $s_i \in \mathbb{Z}$. Dieses Produkt kann man mod N_2 nach Potenzen von x ordnen.

Jede Konjugation mit einem Element $x \in G$ induziert einen Automorphismus in G/N_2 und daher auch in N/N_2 . Da N/N_2 kommutativ ist, bilden die Endomorphismen von N/N_2 einen Ring.

Betrachtet man den von den Konjugationen erzeugten Unterring, dann bedeutet

$$\bigwedge_{y \in N} \bigwedge_{x \in G} w(y, x) = 1 \quad \text{mod } N_2$$

bezogen auf den Endomorphismenring, daß $F(x) = 0$ ist, wobei $F(x)$ den Endomorphismus bezeichnet, der auf y angewendet wird und im obigen Fall $(*)$ durch

$$F(x) = \sum_i x^{s_i}$$

beschrieben wird.

Beispiel: Wenn $F(x) = x^{-1}$ ist, wird dadurch die Abbildung beschrieben, die dem Element $y \in N$ das Element

$$y^{x^{-1}} = y^x y^{-1} = x^{-1} y x y^{-1} = [x, y^{-1}]$$

zuordnet.

Das Problem wird also auf die Bestimmung gewisser Elemente $F(x)$ aus dem Gruppenring $\mathbb{Z}\langle x \rangle$ zurückgeführt. In der neuen Schreibweise lautet dann die Bedingung (I):

$$\bigwedge_{y \in N} \bigwedge_{x \in G} y^{F(x)} \in N_2$$

Der Kreis der in Frage kommenden Gruppenelemente $F(x)$ wird durch die Eigenschaft

$$\bigwedge_{y \in N} \bigwedge_{x \in G} y^{F(x)} \in N_2 \implies \bigwedge_{y \in N} \bigwedge_{x \in G} \bigwedge_{i \in \mathbb{Z}} y^{F(x^i)} \in N_2$$

eingeeengt. Denn bezogen auf den Endomorphismenring von N/N_2 heißt das, daß für alle $i \in \mathbb{Z}$ mit $F(x) = 0$ auch $F(x^i) = 0$ ist.

Es sind also die Ideale in $\mathbb{Z}\langle x \rangle$ gesucht, die mit einem Element $F(x)$ auch alle Elemente $F(x^i)$, $i \in \mathbb{Z}$, enthalten. Dabei kann man sich auf solche Elemente $F(x)$ beschränken, für die $F(1) = 0$ ist, da auch

$$\bigwedge_{y \in N} w(y, 1) \in N_2$$

sein soll.

Die Lösung des Problems vereinfacht sich wesentlich, wenn man einen Primzahlexponenten p für den Normalteiler N vorschreibt, da dann die Fragestellung auf den Gruppenring $\mathbb{Z}_p\langle x \rangle$ bezogen wird. Es wirkt sich hierbei erleichternd aus,

daß $\mathbb{Z}_p$ ein Körper ist.

Aus Gründen der Bequemlichkeit werden im folgenden die Betrachtungen in dem auf natürliche Weise in den Gruppenring $\mathbb{Z}_p\langle x \rangle$ (bzw. $\mathbb{Z}\langle x \rangle$) eingebetteten Polynomring $\mathbb{Z}_p[x]$ (bzw. $\mathbb{Z}[x]$) angestellt.

Die so gewonnenen Ergebnisse lassen sich im allgemeinen sehr schnell auf den jeweiligen Gruppenring übertragen.

Bezeichnung: Als ein Ideal I mit der Eigenschaft E aus einem Gruppen- bzw. Polynomring bezeichnen wir im folgenden jedes Ideal, das mit einem Element $F(x)$ auch jedes Element $F(x^i)$ mit $i \in \mathbb{Z}$, bzw, $i \in \mathbb{N}$, enthält.

Da der Ring $\mathbb{Z}_p[x]$ Hauptidealring ist, werden die Ideale I mit der Eigenschaft E von dem g.g.T. aller Polynome $F(x^i)$, $i \in \mathbb{N}$, erzeugt. Für diesen g.g.T. beweisen wir den

Hilfssatz 3: Wenn in dem Ring $\mathbb{Z}_p[x]$ das Polynom $P(x)$ g.g.T. von Polynomen $F(x^i)$, $i \in \mathbb{N}$, ist, dann ist für alle Zahlen $m \in \mathbb{N}$ das Polynom $P(x^m)$ g.g.T. der Polynome $F(x^{im})$, $i \in \mathbb{N}$, und für alle $m \in \mathbb{N}$ teilt $P(x)$ das Polynom $P(x^m)$.

Beweis: $P(x)$ ist g.g.T. der Polynome $F(x^i)$. Da $\mathbb{Z}_p[x]$ Hauptidealring ist, gibt es für $P(x)$ eine eindeutige Darstellung

$$P(x) = \sum_j f_j(x) F(x^j),$$

wobei nur endlich viele Summanden auftreten und die $f_j(x)$ geeignete Polynome aus $\mathbb{Z}_p[x]$ sind.

Nun existiert eine bijektive Abbildung von $\mathbb{Z}_p[x]$ auf $\mathbb{Z}_p[x^m]$ und es ist

$$P(x^m) = \sum_j f_j(x^m) F(x^{jm}).$$

Also enthält $P(x^m)$ den g.g.T. der $F(x^{im})$ und daher auch den der $F(x^i)$.

Da außerdem die Teilerbeziehung

$$P(x) \mid F(x^i)$$

übertragen wird auf

$$P(x^m) \mid F(x^{im}),$$

ist $P(x^m)$ g.g.T. der Polynome $F(x^{im})$.

Damit ist aber auch bewiesen, daß für alle $m \in \mathbb{N}$ $P(x)$ das Polynom $P(x^m)$ teilt.

//

Diese Eigenschaft des Erzeugenden eines Ideals I mit E verwenden wir, um seine Gestalt zu bestimmen.

Satz 2: Gilt für ein Polynom $P(x)$ aus $\mathbb{Z}_p[x]$

$$\bigwedge_{m \in \mathbb{N}} P(x) \mid P(x^m),$$

dann hat das Polynom die Gestalt

$$P(x) = \prod_k \bar{\alpha}_k^{s_k}(x), \quad (k, p) = 0,$$

wobei $\bar{\alpha}_k(x)$ das k -te Kreisteilungspolynom ist. Tritt in dem Produkt ein Polynom $\bar{\alpha}_k(x)$ auf, dann auch jedes Polynom $\bar{\alpha}_d(x)$, wenn d Teiler von k ist. Außerdem ist stets $s_d \geq s_k$.

Beweis: Es gibt für jedes $m \in \mathbb{N}$ ein Polynom $f_m(x)$ aus $\mathbb{Z}_p \langle x \rangle$ mit $P(x^m) = f_m(x)P(x)$.

Wenn daher a eine t -fache Nullstelle von $P(x)$ ist, dann muß auch a^m eine mindestens t -fache Nullstelle sein.

Da aber der Grad von $P(x)$ endlich ist, muß für eine Zahl $k \in \mathbb{N}$ die Potenz a^k gleich 1 werden, und es muß ein kleinstes k dieser Art geben. Das heißt, mit a sind auch alle Potenzen a^s , $1 \leq s \leq k$, Nullstellen von $P(x)$.

Diese sind aber die Nullstellen des Polynoms $1-x^k$. Daher ist $P(x)$ Teiler einer gewissen Kollektion von Polynomen $(1-x^k)^i$, $i \in \mathbb{N}$, und Vielfaches des k.g.V. dieser Kollektion. Schreibt man $P(x)$ als Produkt von Kreisteilungspolynomen $\Phi_k(x)$ und berücksichtigt, daß für eine t -fache Nullstelle a von $P(x)$ jede Potenz a^m eine mindestens t -fache Nullstelle sein muß, erhält man die Bedingung, daß aus $d|k$ stets $s_d \geq s_k$ folgen muß. Also hat $P(x)$ die behauptete Form.

//

Für den Gruppenring $\mathbb{Z}_p \langle x \rangle$ erhalten wir für ein Ideal I mit E dieselbe Darstellung.

Satz 2': Gilt für ein Element $P(x)$ aus $\mathbb{Z}_p \langle x \rangle$

$$\bigwedge_{m \in \mathbb{Z}} P(x) \mid P(x^m),$$

dann hat $P(x)$ die Gestalt

$$P(x) = \prod_k \Phi_k^{s_k}(x),$$

wobei die in dem Produkt auftretenden Polynome dieselben Eigenschaften haben wie in Satz 2.

Beweis: Das Ideal

$$I = \left\langle \prod_k \mathbb{D}_k^{s_k(x)} \right\rangle$$

sei jetzt aus $\mathbb{Z}_p \langle x \rangle$. Wenn für alle $m \in \mathbb{Z}$ das Polynom $P(x^m)$ von $P(x)$ geteilt wird, hat das Ideal I die Eigenschaft E.

Für $m \in \mathbb{N}$ und $m=0$ gilt nach Voraussetzung, daß $P(x)$ das Polynom $P(x^m)$ teilt.

Sei also $m \in \mathbb{Z} \setminus \mathbb{N}$ und $m \neq 0$.

Das Polynom $P(x)$ läßt sich schreiben als Quotient zweier Produkte von geeigneten Polynomen

$$(1 - x^{k_i}),$$

wobei die k_i so zu wählen sind, daß alle Bedingungen von Satz 2 erfüllt werden.

Daher gibt es zu jeder negativen ganzen Zahl m eine positive ganze Zahl M und es ist

$$P(x^m) = \pm x^{-M} P(x^{-m}),$$

wobei $P(x^{-m})$ aus $\mathbb{Z}_p[x]$ ist.

Das heißt, für alle $m \in \mathbb{Z}$ ist $P(x^m)$ in dem von $P(x)$ in $\mathbb{Z}_p \langle x \rangle$ erzeugten Ideal.

Sei nun umgekehrt I ein Ideal in $\mathbb{Z}_p \langle x \rangle$ mit der Eigenschaft E.

Zu jedem Element $F(x) \in I$ gibt es eine natürliche Zahl M mit

$$F(x) = x^{-M} F'(x),$$

wobei $F'(x)$ aus $I \cap \mathbb{Z}_p[x]$ ist. Auf $F'(x)$ kann man wieder die Methoden von Satz 2 anwenden; d.h. das Ideal I wird von einem Element $P(x)$ der angegebenen Gestalt erzeugt.

//

Beispiele: Die hier aufgeführten Polynome sind aus $\mathbb{Z}_5\langle x \rangle$.

$$P_1(x) = (x^2-1)(x^3-1)(x^6-1) = \bar{a}_1^3(x)\bar{a}_2^2(x)\bar{a}_3^2(x)\bar{a}_6(x)$$

$$P_2(x) = \frac{(x^2-1)(x^3-1)(x^6-1)}{x-1} = \bar{a}_1^2(x)\bar{a}_2^2(x)\bar{a}_3^2(x)\bar{a}_6(x)$$

$$P_3(x) = \frac{(x^2-1)(x^3-1)(x^6-1)}{(x-1)^2} = \bar{a}_1(x)\bar{a}_2^2(x)\bar{a}_3^2(x)\bar{a}_6(x)$$

Die Polynome $P_1(x)$ und $P_2(x)$ erfüllen die Bedingungen von Satz 2. Die von ihnen erzeugten Ideale haben daher die Eigenschaft E.

In dem Polynom $P_3(x)$ dagegen tritt $\bar{a}_1(x)$ nur in der ersten, $\bar{a}_2(x)$ dagegen in der zweiten Potenz auf. Dies hat zur Folge, daß zum Beispiel $P_3(x)$ nicht $P_3(x^2)$ teilt.

Die Aussage von Satz 2 läßt sich für gewisse Fälle verallgemeinern, in denen der Polynomring kein Hauptidealring ist. Betrachten wir den in dem Gruppenring $\mathbb{Z}_{p^n}\langle x \rangle$ enthaltenen Polynomring $\mathbb{Z}_p[x]$, $n \in \mathbb{N}$.

Satz 3: Wenn ein Ideal I aus $R := \mathbb{Z}_{p^n}[x]$, $n \in \mathbb{N}$, die Eigenschaft E hat, dann gilt:

$$I = \left\langle p^{j-1}P_j(x) + \sum_{s=j}^{n-1} p^s w_{j,s}(x) \mid 1 \leq j \leq n \right\rangle$$

$$(w_{n,n-1}(x) = 0)$$

Dabei hat jedes Polynom $P_j(x)$, $1 \leq j \leq n$, die Gestalt des Polynoms $P(x)$ aus Satz 1 und es gilt:

$$P_1(x) \mid P_j(x) \quad \text{für } 1 \leq j \leq n \quad \text{und}$$

$$\text{grad } w_{j,s}(x) < \text{grad } P_{s+1}(x) \quad \text{für } 1 \leq j \leq n-1.$$

Beweis: Für $n=1$ wurde die Aussage in Satz 2 bewiesen.

Angenommen, sie ist wahr für $n-1$.

Da, betrachtet als R -Modul,

$$p^{n-1} R \cong \mathbb{Z}_p[x]$$

ist, ist

$$I \cap p^{n-1} R = p^{n-1} \langle P_n(x) \rangle,$$

wobei $P_n(x)$ von der Gestalt des Polynoms $P(x)$ aus Satz 2 ist.

Nach Induktionsannahme gilt

$$I + p^{n-1}R / p^{n-1}R = \left\langle p^{j-1}P_j(x) + \sum_{s=j}^{n-2} p^s w_{j,s}(x) \mid 1 \leq j \leq n-1 \right\rangle \mod p^{n-1}R. \quad (w_{n-1,n-2}(x)=0)$$

Also ist nach dem Noetherschen Isomorphiesatz

$$I = \left\langle p^{j-1} P_j(x) + \sum_{s=j}^{n-1} p^s w_{j,s}(x) \mid 1 \leq j \leq n \right\rangle. \quad (w_{n,n-1}(x)=0)$$

Da das Ideal

$$J := \left\langle p^{n-2} P_{n-1}(x) + p^{n-1} w_{n-1,n-1}(x), p^{n-1} P_n(x) \right\rangle$$

in I enthalten ist, ist

$$pJ \subseteq I \cap p^{n-1}R.$$

Daher teilt $P_n(x)$ das Polynom $P_{n-1}(x)$. Zusammen mit der Induktionsannahme erhält man:

$$P_1(x) \mid P_j(x) \quad \text{für } 1 \leq j \leq i \leq n$$

Nach Induktionsannahme ist

$$\text{grad } w_{j,s}(x) < \text{grad } P_{s+1}(x) \quad \text{für } j \leq s \leq n-2.$$

Wenn $\text{grad } w_{j,n-1}(x) \geq \text{grad } P_n(x)$, $1 \leq j \leq n-1$, ist, gibt es Polynome $r_{j,n-1}(x)$ und $w'_{j,n-1}(x)$, derart daß gilt:

$$w_{j,n-1}(x) = r_{j,n-1}(x) P_n(x) + w'_{j,n-1}(x),$$

wobei $\text{grad } w'_{j,n-1}(x) < \text{grad } P_n(x)$ ist. Es interessieren also nur Polynome $w_{j,s}(x)$ mit

$$\text{grad } w_{j,s}(x) < \text{grad } P_{s+1}(x)$$

für $1 \leq j \leq s \leq n-1$.

//

Im Gruppenring $\mathbb{Z}_n \langle x \rangle$ gilt für ein Ideal I mit der Eigenschaft E folgende Aussage:

Satz 3': Wenn ein Ideal I aus $R := \mathbb{Z}_n \langle x \rangle$, $n \in \mathbb{N}$, die Eigenschaft E hat, dann gilt:

$$I = \left\langle \begin{array}{l} p^{j-1} P_j(x) + \sum_{s=j}^{n-1} p^s w_{j,s}(x), \\ p^{j-1} P_j(x^{-1}) + \sum_{s=j}^{n-1} p^s w_{j,s}(x^{-1}) \end{array} \right| \quad 1 \leq j \leq n \right\rangle$$

$$(w_{n,n-1}(x) = 0)$$

Dabei haben die Polynome $P_j(x)$ und $w_{j,s}(x)$ die Eigenschaften der Polynome aus Satz 3. $P_j(x^{-1})$ und $w_{j,s}(x^{-1})$ sind die Elemente aus $\mathbb{Z}_n \langle x \rangle$, die aus den Polynomen $P_j(x)$ und $w_{j,s}(x)$ durch die Abbildung $x \mapsto x^{-1}$ entstehen.

Beweis: Wie man leicht nachrechnet hat das so erzeugte Ideal I die Eigenschaft E .

Sei umgekehrt ein Ideal I aus R mit der Eigenschaft E gegeben. Jedes Element aus I läßt sich als Summe zweier Elemente schreiben, von denen das eine aus $\mathbb{Z}_p[x]$ und das andere aus $\mathbb{Z}_p[x^{-1}]$ ist.

Das Ideal I hat also die angegebene Gestalt.

//

Mit Satz 3' hat man die Möglichkeit, jedes Ideal I aus dem Gruppenring $\mathbb{Z}\langle x \rangle$ mit der Eigenschaft E zu beschreiben.

Satz 4: Wenn ein Ideal I aus dem Gruppenring $\mathbb{Z}\langle x \rangle$ die Eigenschaft E hat, dann gibt es eine natürliche Zahl n mit der eindeutigen Primzahlzerlegung

$$n = \prod_{i=1}^r p_i^{n_i}$$

und ein Polynom $P_{0,0}(x)$ mit den Eigenschaften des Polynoms $P(x)$ aus Satz 2, die folgende Darstellung von I liefern.

$$I = \left\langle n P_{0,0}(x), M_{i,j}(x), M_{i,j}(x^{-1}) \mid 1 \leq i \leq r, 1 \leq j \leq n_i \right\rangle$$

wobei

$$M_{i,j}(x) = p_i^{j-1} P_{i,j}(x) + \sum_{s=j}^{n_i-1} p_i^s w_{i,j,s}(x) + n w_{i,j}(x)$$

ist. Alle in der Darstellung auftretenden Polynome haben dieselben Eigenschaften wie die entsprechenden in Satz 3' und es gilt:

$$\begin{aligned} \text{grad } w_{i,j,s}(x) &< \text{grad } P_{i,s+1}(x) && \text{für } 1 \leq j \leq s \leq n_i, 1 \leq i \leq r \\ P_{0,0}(x) &\mid P_{i,h}(x) \mid P_{i,k}(x) && \text{für } 1 \leq k \leq h \leq n_i, 1 \leq i \leq r \end{aligned}$$

Beweis: Betrachte den in $\mathbb{Z}\langle x \rangle$ enthaltenen Polynomring $\mathbb{Z}[x]$.
 I sei ein in $\mathbb{Z}[x]$ enthaltenes Ideal mit der Eigenschaft E.

Da $\mathbb{Z}[x]$ ein Noetherscher Ring ist, läßt sich I endlich erzeugen:

$$I = \langle f_1(x), \dots, f_t(x) \rangle$$

Bette $\mathbb{Z}[x]$ in $\mathbb{Q}[x]$ ein. In $\mathbb{Q}[x]$ ist I Hauptideal. Es existiert also ein Polynom $P_{0,0}(x)$ mit den Eigenschaften des Polynoms $P(x)$ aus Satz 2 und in $\mathbb{Q}[x]$ ist

$$I = \langle P_{0,0}(x) \rangle.$$

Es gibt daher eine natürliche Zahl n und

$$\bigwedge_{1 \leq i \leq r} n P_{0,0}(x) L_i(x) = f_i(x)$$

mit geeignetem Polynom $L_i(x)$ aus $\mathbb{Q}[x]$.
 Das heißt, für das Ideal I gilt:

$$I \cap n \mathbb{Z}[x] = \langle n P_{0,0}(x) \rangle$$

Nach dem Noetherschen Isomorphiesatz ist

$$I + n \mathbb{Z}[x] / n \mathbb{Z}[x] \cong I / I \cap n \mathbb{Z}[x]$$

Das Ideal

$$I + n \mathbb{Z}[x] / n \mathbb{Z}[x]$$

ist enthalten in dem Ring

$$\mathbb{Z}[x] / n \mathbb{Z}[x] \cong \mathbb{Z}_n[x].$$

Da für je zwei teilerfremde Zahlen r und s aus $\mathbb{N}$

$$\mathbb{Z}_{rs}[x] \cong \mathbb{Z}_r[x] + \mathbb{Z}_s[x]$$

ist, gilt

$$\mathbb{Z}_n[x] \cong \sum_{i=1}^r \mathbb{Z}_{\frac{n}{p_i}}[x].$$

In jedem der Polynomringe $\mathbb{Z}_{\frac{n}{p_i}}[x]$ ist die Gestalt des

Ideals I bekannt.

Mit den Methoden, die beim Beweis der Sätze 3 und 3' angewandt wurden, erhält man auf diese Weise die angegebene Gestalt von I und die Eigenschaften der auftretenden Polynome.

//

Die Bestimmung der in den Sätzen 3, 3' und 4 auftretenden Polynome $w_{i,j,s}(x)$ bzw. $w_{j,s}(x)$ ist im allgemeinen sehr schwierig. In einigen Fällen gelingt dies jedoch mit relativ geringem Aufwand. Man kann nämlich beweisen, daß diese Polynome gleich 0 sind, wenn die Polynome $P_{i,j}(x)$ bzw. $P_j(x)$ bestimmte Eigenschaften haben.

Es genügt, nur die Polynome $w_{j,s}(x)$ aus Satz 3 zur Untersuchung heranzuziehen. Die Ergebnisse lassen sich ohne weiteres auf Satz 4 ausdehnen.

Zum Beweis von Satz 5 benötigt man folgenden Satz aus der Zahlentheorie:

Hilfssatz 4: Für Polynome $f(x)$ und $g(x)$ aus dem Ring $\mathbb{Z}[x]$ gilt:

Ist a eine modulo der Primzahl p einfache Nullstelle von $f(x)$, so gibt es mod p^{k+1} eine Nullstelle $a+p^k t$, t geeignet gewählt, von $f(x)+p^k g(x)$, wenn $k > 0$ ist.

Beweis: Wenn a eine einfache Nullstelle von $f(x) \pmod p$ ist, ist $f'(a) \not\equiv 0 \pmod p$ und

$$f(a+p^k t) = f(a) + t p^k f'(a) \pmod{p^{k+1}}.$$

Es ist deshalb

$$\begin{aligned} f(a+p^k t) + p^k g(a+p^k t) &= f(a) + p^k t f'(a) + p^k g(a) \pmod{p^{k+1}} \\ &= p^k (t f'(a) + g(a)) \pmod{p^{k+1}}. \end{aligned}$$

Da $f'(a) \pmod p$ ungleich Null ist, ist für $t = -g(a)/f'(a)$ die Zahl $a+p^k t$ eine Nullstelle von $f(x) + p^k g(x) \pmod{p^{k+1}}$.

//

Satz 5: Wenn ein Ideal I aus $\mathbb{Z}_n[x]$, $n \in \mathbb{N}$, die Eigenschaft E hat und die Polynome $P_j(x)$, $1 \leq j \leq n$, $\pmod p$ nur einfache Nullstellen besitzen, dann gilt:

$$I = \left\langle p^{j-1} P_j(x) \mid 1 \leq j \leq n \right\rangle$$

Beweis: Der Beweis wird der Einfachheit halber im Polynomring $\mathbb{Z}_n[x]$ geführt. Die Übertragung auf den Gruppenring erfolgt genauso wie beim Beweis von Satz 2' und wird deshalb nicht durchgeführt.

Im Fall $n=1$ haben wir die Aussage von Satz 2'.

Angenommen, $w_{j,s}(x) = 0$ für $1 \leq j \leq n-2$ und $1 \leq s \leq n-2$.

Es genügt nachzuweisen, daß $w_{n-1,n-1}(x) = 0$ ist, da dann mit derselben Methode sukzessiv gezeigt werden kann, daß auch $w_{j,n-1}(x) = 0$, $1 \leq j \leq n-2$, ist.

Alle Nullstellen von $P_{n-1}(x)$ und damit auch von $P_n(x)$ seien einfach. Dann gibt es mod p^2 zu jeder Nullstelle a von $P_{n-1}(x)$ eine Nullstelle $a+pt$ von

$$h'(x) := P_{n-1}(x) + p w_{n-1, n-1}(x);$$

d.h. $h(x) := p^{n-2} h'(x)$ läßt sich schreiben als

$$h(x) = p^{n-1} \prod_i (x - (a_i + pt_i)),$$

wobei die a_i die Nullstellen von $P_{n-1}(x)$ sind und die Existenz der t_i durch Hilfssatz 4 gesichert ist.

Mit b ist auch jede Potenz b^m Nullstelle von $P_n(x)$ und mod p ist auch $b+pt_b$ (t_b existiert nach Hilfssatz 4) und jede Potenz $(b + pt_b)^m$ Nullstelle von $P_n(x)$.

Die Nullstellen von $P_n(x)$ sind alle einfach. Jede Nullstelle mod p von $P_n(x)$ ist mod p Nullstelle von $P_{n-1}(x)$ und daher mod p^2 Nullstelle von $h'(x)$. Deshalb ist

$$h(x) = p^{n-2} P_n(x) \prod_i^* (x - (a_i + pt_i)).$$

//

Einen weiteren Fall, in dem die Polynome $w_{j,s}(x)$ aus Satz 3 vernachlässigt werden können erhält man, wenn der Grad des in der Darstellung von I auftauchenden Polynoms $P_1(x)$ gewissen Beschränkungen unterworfen wird.

Es gilt nämlich für alle Primzahlen $p \neq 2$:

Hilfssatz 5: Wenn ein Ideal I aus $\mathbb{Z}_{p^2}[x]$ die Eigenschaft E hat und

$$I = \langle P_1(x) + pw(x), pP_2(x) \rangle$$

ist, gilt:

Wenn für natürliche Zahlen r und s mit $1 \leq r \leq s \leq p-1$ $(x-a)^s$ maximaler Teiler von $P_1(x)$ und $(x-a)^r$ Teiler von $P_2(x)$ ist, dann ist $\text{mod } p$ $(x-a)^r$ Teiler von $w(x)$.

Beweis: $r = 1$:

Setze $P_1(x) = (x-a)^s T(x)$ mit $T(a) \neq 0$.

Da a Nullstelle von $P_1(x)$ ist, gibt es eine natürliche Zahl n mit

$$a^n = 1.$$

Wähle $k \in \mathbb{N}$ so, daß

$$m := kn + 1 \not\equiv 1 \pmod{p}$$

ist. Dann gilt:

$$\begin{aligned} p(w(x) \frac{P_1(x^m)}{P_1(x)} - w(x^m)) &= p(w(x) (\frac{x^m - a}{x - a})^s \frac{T(x^m)}{T(x)} - w(x^m)) = \\ &= p(w(x) (\sum_{i=1}^m \binom{m}{i} (x-a)^{i-1})^s \frac{T(x^m)}{T(x)} - w(x^m)) = pf(x)P_2(x) \end{aligned}$$

mit einem geeigneten Polynom $f(x)$ aus $\mathbb{Z}_{p^2}[x]$.

Setzt man die Nullstelle a ein, erhält man

$$w(a) (\sum_{i=1}^m \binom{m}{i} (a-a)^{i-1})^s \frac{T(a)}{T(a)} - w(a) = w(a)(m^s - 1) = 0 \pmod{p},$$

da $P_2(a) = 0$ ist.

Weil $m \not\equiv 1 \pmod{p}$ gewählt wurde, ist $m^s \not\equiv 1$, also $w(a) = 0$; d.h. $x-a$ teilt das Polynom $w(x)$.

Sei nun $r > 1$ und die Behauptung für $r-1$ wahr.

Wähle $k \in \mathbb{N}$ so, daß

$$m: = kn + 1 \neq \begin{cases} 0 \\ 1 \end{cases} \pmod{p}$$

ist. Dann gilt wie im Fall $r=1$, wenn man

$$w(x) = (x-a)^{r-1}v(x) \quad \text{und} \quad P_2(x) = (x-a)^{r-1}R(x)$$

(mit geeigneten Polynomen $v(x)$ und $R(x)$) setzt,

$$\begin{aligned} p(w(x) \frac{P_1(x^m)}{P_1(x)} - w(x^m)) &= \\ &= p((x-a)^{r-1}v(x) (\sum_{i=1}^m \binom{m}{i} (x-a)^{i-1})^s \frac{T(x^m)}{T(x)} - (x^m-a)^{r-1}v(x^m)) = \\ &= p((x-a)^{r-1}(v(x) (\sum_{i=1}^m \binom{m}{i} (x-a)^{i-1})^s \frac{T(x^m)}{T(x)} - \\ &\quad - (\sum_{i=1}^m \binom{m}{i} (x-a)^{i-1})^{r-1}v(x^m))) = pf(x)(x-a)^{r-1}R(x) \end{aligned}$$

mit geeignetem Polynom $f(x)$ aus $\mathbb{Z}_{p^2}[x]$.

Durch Einsetzen der Nullstelle a erhält man

$$\begin{aligned} v(a)m^s \frac{T(a^m)}{T(a)} - m^{r-1} v(a^m) &= v(a)(m^s - m^{r-1}) = \\ &= v(a)m^{r-1}(m^{s-(r-1)} - 1) = 0 \pmod{p}, \end{aligned}$$

da $R(a) = 0$ ist.

$m^{s-(r-1)} \neq 1 \pmod{p}$ und $m^{r-1} \neq 0 \pmod{p}$, da

$m \neq \begin{cases} 0 \\ 1 \end{cases} \pmod{p}$ gewählt wurde und $r > 1$ und $s \leq p-1$

sind. Also ist $v(a) = 0 \pmod{p}$ und daher $w(x)$ teilbar durch $(x-a)^r$.

//

Satz 6: Wenn ein Ideal I aus $\mathbb{Z}_{p^n}\langle x \rangle$, $n \in \mathbb{N}$, die Eigenschaft E hat und die Vielfachheit jeder Nullstelle von $P_1(x)$ kleiner oder gleich $p-1$ ist, dann gilt:

$$I = \left\langle p^{j-1} P_j(x) \mid 1 \leq j \leq n \right\rangle$$

Beweis: Der Beweis wird wieder aus Gründen der Bequemlichkeit für Ideale I aus dem Polynomring $\mathbb{Z}_{p^n}[x]$ geführt.

Für $p=2$ wurde die Behauptung in Satz 5 bewiesen.

Sei also $p \neq 2$. Für $n=1$ haben wir die Aussage von Satz 2'. Angenommen, die Polynome $w_{j,s}(x)$ sind für

$1 \leq j \leq n-2$ und $1 \leq s \leq n-2$ gleich Null. In $\mathbb{Z}_{p^n}[x]$ hat dann I die Gestalt

$$I = \left\langle p^{j-1} P_j(x) + p^{n-1} w_{j,n-1}(x) \mid 1 \leq j \leq n \right\rangle.$$

Die Überlegungen aus Hilfssatz 5 kann man nun auf

$$p^{n-1} \left(w_{j,n-1} \frac{P_j(x^m)}{P_j(x)} - w_{j,n-1}(x) \right) \in \left\langle p^{n-1} P_n(x) \right\rangle$$

für $1 \leq j \leq n-1$ und geeignet gewähltes $m \in \mathbb{N}$ anwenden und erhält, daß das Ideal I die angegebene Gestalt hat.

//

Mit Hilfe der Sätze 5 und 6 erhält man eine große Klasse von Idealen mit der Eigenschaft E , in deren Erzeugenden die Polynome $w_{j,s}(x)$, über die man so wenig Informationen hat, nicht auftreten.

Im allgemeinen kann man diese Polynome jedoch nicht vernachlässigen, wie das folgende Beispiel zeigt.

Beispiel: Betrachte das Ideal

$$I = \langle (x-1)^3 + p(x-1), (x^{-1}-1)^3 + p(x^{-1}-1), p(x-1)^2 \rangle$$

mit der Eigenschaft E , gebildet in $\mathbb{Z}_p[x]$.

In diesem Fall haben die Polynome

$$P_1(x) = (x-1)^3 \quad \text{und} \quad P_2(x) = (x-1)^2$$

die mehrfache Nullstelle 1. Außerdem ist in $P_1(x)$ für $p \neq 3$ die Vielfachheit der Nullstelle 1 größer als $p-1$.

Daher kann für $p \neq 3$, wie die folgende Überlegung zeigt, das Polynom $w(x) = x-1$ nicht vernachlässigt werden. (Dasselbe Ergebnis erhält man mit einer analogen Überlegung für das Polynom $w(x^{-1}) = x^{-1}-1$).

Jedes Polynom $P(x) \in I \cap \mathbb{Z}_p[x]$ wird folgendermaßen gebildet:

$$P(x) = f(x)((x-1)^3 + p(x-1)) + g(x)p(x-1)^2$$

mit geeigneten Polynomen $f(x)$ und $g(x)$.

Für beliebiges $n \in \mathbb{N}$ ist

$$\begin{aligned} P(x^n) &= f(x^n)((x^n-1)^3 + p(x^n-1)) + g(x^n)p(x^n-1)^2 = \\ &= f(x^n)\left(\frac{x^n-1}{x-1}\right)^3((x-1)^3 + p(x-1)) + f(x^n)p(x-1)\left(\left(\frac{x^n-1}{x-1}\right) - \left(\frac{x^n-1}{x-1}\right)^3\right) + \\ &+ g(x^n)\left(\frac{x^n-1}{x-1}\right)^2 p(x-1)^2. \end{aligned}$$

Für jedes $n \in \mathbb{N}$ soll $P(x^n) \in I$ sein. Dies ist aber nur dann der Fall, wenn der Ausdruck

$$\frac{x^n-1}{x-1} - \left(\frac{x^n-1}{x-1}\right)^3$$

durch $x-1$ teilbar ist; d.h. wenn $p \neq 3$ ist.

Um zu demonstrieren, wie unübersichtlich die Form der Polynome $w_{j,s}(x)$ sein kann, wenn die Voraussetzungen der Sätze 5 und 6 nicht erfüllt sind, wird die Gestalt des Polynoms $w_{1,1}(x)$ für ein Ideal mit der Eigenschaft E aus dem Polynomring $\mathbb{Z}_p[x]$ angegeben.

In dieser Darstellung tritt die Funktion $\ln x$ auf. Darunter ist modulo einer gewissen Potenz von $x-1$, die immer angegeben wird, die Taylorreihenentwicklung

$$\ln x = \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i} (x-1)^i$$

zu verstehen. Für die Glieder dieser Reihe gilt folgende Aussage:

Hilfssatz 6: Für die Glieder der Taylorentwicklung

$$\ln(1+(x-1)) = \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i} (x-1)^i$$

der Logarithmusfunktion gilt:

$$\bigwedge_{n \in \mathbb{N}} \bigwedge_{r \in \mathbb{N}} \sum_{i=1}^r \frac{(-1)^{i+1}}{i} (x^n-1)^i = n \sum_{i=1}^r \frac{(-1)^{i+1}}{i} (x-1)^i \mod (x-1)^{r+1}$$

Beweis: Der Beweis erfolgt durch Vergleich der beiden Potenzreihen

$$\begin{aligned} \ln(1+(x^n-1)) &= \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i} (x^n-1)^i = \\ &= \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i} \left(\sum_{j=1}^n \binom{n}{j} (x-1)^j \right)^i \end{aligned}$$

$$\text{und } n \ln(1+(x-1)) = n \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i} (x-1)^i.$$

Diese sind gleich. Also haben sie gleiche Koeffizienten, woraus die Behauptung folgt.

//

Satz 7: Das Ideal

$$I = \left\langle P_1(x) + pR \frac{P_1(x)}{(x^r-1)^p} \ln x^r, pP_2(x) \right\rangle$$

aus dem Polynomring $\mathbb{Z}_p[x]$ hat die Eigenschaft E, wenn

$$\text{grad } P_1(x) - r(p-1)+1 \leq \text{grad } P_2(x) \leq \text{grad } P_1(x)$$

ist.

Dabei ist $R \in \mathbb{Z}$ beliebig und $(x^r-1)^p$ Teiler von $P_1(x)$. Die Reihendarstellung von $\ln x$ bricht ab, wenn

$$\text{grad } p \frac{P_1(x)}{(x^r-1)^p} \ln x^r = \text{grad } pP_2(x)$$

ist.

Beweis: Sind die Vielfachheiten aller Nullstellen von $P_1(x)$ kleiner oder gleich $p-1$, muß $R=0$ sein, wie in Satz 6 bewiesen wurde.

Wenn $P_1(x)$ eine Nullstelle a mit der Vielfachheit $k \geq p$ hat, muß es einen Teiler $(x^r-1)^p$ von $P_1(x)$ geben, der a als Nullstelle hat.

Es gilt daher

$$\begin{aligned} \bigwedge_{n \in \mathbb{N}} P_1(x^n) + pR \frac{P_1(x^n)}{(x^{nr}-1)^p} \ln x^{nr} &= \\ &= \frac{P_1(x^n)}{P_1(x)} (P_1(x) + pR \frac{P_1(x)}{(x^r-1)^p} \ln x^r) - \end{aligned}$$

$$\begin{aligned}
 &= pR \frac{P_1(x^n)P_1(x)}{P_1(x)(x^r-1)^p} \ln x^r + pR \frac{P_1(x^n)}{(x^{nr}-1)^p} \ln x^{nr} = \\
 &= \frac{P_1(x^n)}{P_1(x)} (P_1(x) + pR \frac{P_1(x)}{(x^r-1)^p} \ln x^r) - \\
 &= pR \left(\left(\sum_{i=1}^n \binom{n}{i} (x^r-1)^{i-1} \right)^p - n \right) \frac{P_1(x^n)}{(x^{nr}-1)^p} \ln x^r
 \end{aligned}$$

Da der zweite Summand in dem Ideal $\langle pP_2(x) \rangle$ liegt, hat das Ideal I die Eigenschaft E ; d.h.

$$\bigwedge_{n \in \mathbb{N}} F(x) \in I \implies F(x^n) \in I.$$

//

Bemerkung: Wenn in Satz 7 das Polynom

$$P_1(x) = (x-1)^p$$

ist, erhält man für das Ideal

$$I = \langle (x-1)^p + pR \ln x, p(x-1)^r \rangle$$

mit $0 \leq r \leq p$. Nun gilt aber

$$\bigwedge_{n \in \mathbb{N}} \binom{p}{n} = (-1)^{n+1} \frac{1}{n} p \pmod{p^2}.$$

Man erhält somit

$$\begin{aligned}
 (x^p-1) - (x-1)^p &= ((x-1)+1)^p - (x-1)^p = \\
 &= \left(\sum_{i=0}^p \binom{p}{i} (x-1)^{i-1} \right) - (x-1)^p = \sum_{i=1}^{p-1} \binom{p}{i} (x-1)^i = \\
 &= \sum_{i=1}^{p-1} p \frac{(-1)^{i+1}}{i} (x-1)^i = p \ln x \pmod{\langle p^2, (x-1)^p \rangle}.
 \end{aligned}$$

Für das Ideal I bedeutet das:

$$I = \langle (x-1)^p + R((x^p-1) - (x-1)^p), p(x-1)^r \rangle,$$

mit einer Zahl $R \in \mathbb{Z}$.

Dies läßt die Vermutung zu, daß in $\mathbb{Z}_p[x]$

$$I = \left\langle p^{j-1}((x-1)^{r_j} + R_j((x^p-1) - (x-1)^p)) \mid 1 \leq j \leq n \right\rangle$$

ist, für gewisse Zahlen $R_j \in \mathbb{Z}$, wobei $r_1 = p$ und $r_1 < r_j$ für $1 \leq j \leq n$ ist.

3. Einbettungsgesetze mit Kommutatoreigenschaften

In Abschnitt 2 wurden die Einbettungsgesetze w bezüglich eines abelschen Normalteilers N einer Gruppe G klassifiziert. Unter diesen Gesetzen w interessieren nun die, die sich auf unser spezielles Problem, d.h. auf Satz 1 anwenden lassen. Wir suchen die Einbettungsgesetze w , für die zusätzlich gilt (Bedingung (II)):

$$\bigwedge_U \bigwedge_V U \trianglelefteq G \wedge V \trianglelefteq G \implies w([U, V], G) \leq [w(U, G), V] [U, w(V, G)] \pmod{[U, V, U] [U, V, V]}$$

Oder anders ausgedrückt:

Es sind die Endomorphismen $F(x)$ abelscher Normalteiler gesucht, für die gilt:

$$\bigwedge_{x \in G} [U, V]^{F(x)} \leq [U^{F(x)}, V] [V, U^{F(x)}] \pmod{[U, V, U] [U, V, V]}$$

Für beliebige Elemente u, v und x aus U, V und G gilt:

$$[u, v]^x = [u^x, v^x];$$

d.h. Konjugation des Kommutators $[u, v]$ mit einem Element $x \in G$ bewirkt die Konjugation jeder einzelnen Komponente des Kommutators mit x .

Man kann also die Konjugation des Kommutators auffassen als die Nacheinanderausführung zweier Operationen x_1 und x_2 , wobei die Operation x_1 Konjugation mit x in der ersten Komponente und die Operation x_2 Konjugation mit x in der zweiten Komponente bewirkt.

In dem Endomorphismus $F(x)$ wird die Ausführung der beiden komponentenweisen Konjugationen verwirklicht, indem man x durch $x_1 x_2$ ersetzt.

Das Problem wird damit auf die Bestimmung gewisser Elemente $F(x_1, x_2)$ aus dem Gruppenring $\mathbb{Z}\langle x_1, x_2 \rangle$ über einer freien abelschen Gruppe $\langle x_1, x_2 \rangle$ vom Rang 2 zurückgeführt.

Läßt sich $F(x_1, x_2)$ schreiben als

$$F(x_1, x_2) = R(x_1, x_2)F(x_1) + S(x_1, x_2)F(x_2),$$

mit gewissen Elementen $R(x_1, x_2)$ und $S(x_1, x_2)$ aus dem Gruppenring $\mathbb{Z}\langle x_1, x_2 \rangle$, dann gilt:

$$\begin{aligned} \bigwedge_{u \in U} \bigwedge_{v \in V} \bigwedge_{x \in G} w([u, v], x) &= [u, v]^{F(x)} = [u, v]^{F(x_1, x_2)} = \\ &= [u, v]^{R(x_1, x_2)F(x_1) + S(x_1, x_2)F(x_2)} = \\ &= [u^{F(x_1)}, v]^{R(x_1, x_2)} [u, v^{F(x_2)}]^{S(x_1, x_2)} \leq \\ &\leq [w(u, x), v] [u, w(v, x)] \mod [U, V, U] [U, V, V] \end{aligned}$$

Bezeichnung: Als ein Ideal I mit der Eigenschaft E' bezeichnen wir jedes Ideal aus dem Gruppenring $\mathbb{Z}\langle x_1, x_2 \rangle$, für das gilt:

$$a) \quad I \subseteq I_{x_1} + I_{x_2}$$

b) Zu jedem Element der Form $P(x_1, x_2) \in I$ gibt es Elemente $f_1(x_1, x_2)$ und $f_2(x_1, x_2)$ aus $\mathbb{Z}\langle x_1, x_2 \rangle$, sodaß

$$P(x_1, x_2) = f_1(x_1, x_2)P(x_1) + f_2(x_1, x_2)P(x_2)$$

ist.

Dabei ist das Ideal I_{x_1} (bzw. I_{x_2}) das in $\mathbb{Z}\langle x_1, x_2 \rangle$ eingebettete Ideal mit der Eigenschaft E aus dem Gruppenring

$R\langle x_1 \rangle$ (bzw. $R\langle x_2 \rangle$). R steht für jeden der Ringe $\mathbb{Z}$ oder $\mathbb{Z}_p^n$ (p ist eine beliebige Primzahl, n eine natürliche Zahl).

Bevor wir dazu übergehen diese Ideale zu bestimmen, soll, wie auf Seite 9 angekündigt, die Umkehrung von Satz 1 bewiesen werden.

Satz 8: Die Bedingung (II) ist notwendig, damit ein Wort w die folgende Eigenschaft hat:

Ist N ein Normalteiler einer Gruppe G , dann gilt:

$$w(N, G) \leq N_2 \implies w(N_2, G) \leq N_3$$

Bemerkung: Daraus folgt, daß die Bedingung (II) auch notwendig ist für die Aussage (B), da diese für alle natürlichen Zahlen i gelten soll.

Beweis von Satz 8: Betrachte die Gruppe

$$G = \left\langle u, v, x \mid \bigwedge_{g \in G} [g, u, u] = [g, v, v] = 1 \wedge \right. \\ \left. \wedge w(u, x) = w(v, x) = 1 \right\rangle,$$

wobei das Wort w die Bedingung (I) erfüllt.

Sei $N := \langle u, v \rangle^G$ und F der auf Seite 10 erklärte Endomorphismus, der durch w beschrieben wird.

Dann ist $N_3 = 1$ und nach Hilfssatz 1

$$w(N, G) \leq N_2.$$

Nach Annahme folgt daraus

$$w(N_2, G) = 1.$$

Das ist aber nur dann der Fall, wenn der Endomorphismus

F , aufgefaßt als Element des Gruppenrings $\mathbb{Z}\langle x_1, x_2 \rangle$, die Eigenschaft

$$(*) \quad F(x_1 x_2) = f_1(x_1, x_2)F(x_1) + f_2(x_1, x_2)F(x_2)$$

hät.

Denn angenommen, F hat nicht die Eigenschaft $(*)$, dann gilt für ein Basiselement

$$[u^{x^i}, v^{x^j}], \quad i \in \mathbb{N}, \quad j \in \mathbb{N} \quad \text{und} \quad i, j < \text{grad } F,$$

von N_2 :

In dem Ausdruck

$$[u^{x^i}, v^{x^j}]^{F(g)} = \prod_{k=0}^{\text{grad } F} [u^{x^i}, v^{x^j}]^{a_k g^k},$$

tritt mindestens ein Faktor (z.B. für $k = k'$) auf, in dem $a_{k'} \neq 0$ ist und $g^{k'}$ auf beiden Komponenten des Kommutators

$$[u^{x^i}, v^{x^j}]$$

gleichzeitig operiert. (Dabei ist a_k der k -te Koeffizient von F und g ein beliebiges Element aus $G \setminus N$.)

Dieser Faktor ist also ungleich 1. Weshalb im Widerspruch zur Voraussetzung auch

$$[u^{x^i}, v^{x^j}]^{F(g)} \neq 1$$

ist.

//

Jedes Element $F(x_1, x_2)$ aus einem Ideal I mit der Eigenschaft E' klassifiziert ein Einbettungsgesetz w , das die Bedingungen (I) und (II) aus Abschnitt 1 erfüllt.

Bei der Suche nach den Erzeugenden der Ideale I mit der Eigenschaft E' gehen wir ähnlich vor wie in Abschnitt 2.

Satz 9: Wenn ein Ideal I aus dem Gruppenring $\mathbb{Z}_p\langle x_1, x_2 \rangle$ die Eigenschaft E' hat, dann haben die Erzeuger der Ideale

$$I_{x_1} \quad \text{bzw.} \quad I_{x_2}$$

die Gestalt

$$P(x_1) = (x_1^k - 1) \quad \text{bzw.} \quad P(x_2) = (x_2^k - 1)$$

mit einer Zahl $k \in \mathbb{N}$.

Beweis: Zunächst wird gezeigt, daß

$$P(x_1) = (x_1^k - 1)^n, \quad k \in \mathbb{N}, \quad n \in \mathbb{N},$$

ist (analog $P(x_2)$).

Sei u eine Nullstelle von $P(x_2)$ (und damit auch von $P(x_1)$), dann ist

$$P(ux_1) = f_1(x_1, u)P(x_1) + f_2(x_1, u)P(u) = f_1(x_1, u)P(x_1).$$

$P(ux_1)$ und $P(x_1)$ haben gleichen Grad. Daher ist $f_1(x_1, u)$ eine Konstante.

Bei geeigneter Erweiterung des Grundkörpers ist $P(x_1)$ zerlegbar in lauter lineare Faktoren $x_1 - u_i$. Diese Faktoren werden in $P(ux_1)$ zu

$$ux_1 - u_i.$$

Ist u eine Nullstelle und u_i eine n -fache Nullstelle, so ist auch $u_i u^{-1}$ eine n -fache Nullstelle von $P(x_1)$.

Durch Verwendung von $u_i u^{-1}$ statt u erhält man, daß auch u , also jede Nullstelle, n -fache Nullstelle ist. Die Nullstellen bilden eine zyklische Gruppe von Einheiten und sind daher genau die Lösungen eines Polynoms $x_1^k - 1$.

Da alle Nullstellen die gleiche Vielfachheit haben, ist

$$P(x_1) = (x_1^k - 1)^n.$$

Es ist noch zu zeigen, daß $n=1$ ist. Zum Beweis kann man annehmen, daß $k=1$ und $n \not\equiv 0 \pmod p$ ist. Sei $n > 1$ und

$$(x_1 x_2 - 1)^n = f_1(x_1, x_2)(x_1 - 1)^n + f_2(x_1, x_2)(x_2 - 1)^n$$

ein Element aus dem Ideal I mit der Eigenschaft E' .

Betrachte das Element

$$(x_1 x_2 - 1)^n (x_1 - 1)^{n-2} \in I.$$

Für dieses Element gilt

$$\begin{aligned} (x_1 x_2 - 1)^n (x_1 - 1)^{n-2} &= \\ &= ((x_1 - 1)(x_2 - 1) + (x_1 - 1) + (x_2 - 1))^n (x_1 - 1)^{n-2} = \\ &= ((x_2 - 1)^n F(x_1, x_2) + n(x_2 - 1)^{n-1}(x_1 - 1) + \\ &+ (x_1 - 1)^2 G(x_1, x_2))(x_1 - 1)^{n-2} = \\ &= (x_2 - 1)^n H(x_1, x_2) + (x_1 - 1)^n K(x_1, x_2) + \\ &+ n(x_2 - 1)^{n-1}(x_1 - 1)^{n-1} \end{aligned}$$

mit geeignet gewählten Polynomen $F(x_1, x_2)$, $G(x_1, x_2)$, $H(x_1, x_2)$ und $K(x_1, x_2)$.

Das heißt, das Element

$$(x_1 x_2 - 1)^n (x_1 - 1)^{n-2}$$

ist für $n > 1$ nicht in dem Ideal I enthalten.
Also muß $n=1$ sein.

//

Dieses Ergebnis wird verallgemeinert auf den Fall des Gruppenrings $\mathbb{Z}_p \langle x_1, x_2 \rangle$.

Satz 10: Wenn ein Ideal I aus dem Gruppenring $\mathbb{Z}_p \langle x_1, x_2 \rangle$ die Eigenschaft E' hat, dann ist

$$I = \left\langle p^{n-i} (x_1^{s_i} - 1), p^{n-i} (x_2^{s_i} - 1) \mid 1 \leq i \leq n \right\rangle$$

$$\text{und } s_i \mid s_j \text{ für } 1 \leq i \leq j \leq n.$$

Beweis: Für $n=1$ wurde die Behauptung in Satz 9 bewiesen.

Angenommen, die Behauptung ist für $n-1$ richtig.
Den Induktionsschluß von $n-1$ nach n führen wir im Polynomring $R := \mathbb{Z}_p[x_1, x_2]$ durch.

Dann ist

$$I \cap p^{n-1} R = p^{n-1} \left\langle x_1^{s_1} - 1, x_2^{s_2} - 1 \right\rangle$$

und

$$I + p^{n-1}R / p^{n-1}R =$$

$$= \left\langle p^{n-i}(x_1^{s_i} - 1), p^{n-i}(x_2^{s_i} - 1) \mid 2 \leq i \leq n \right\rangle \bmod p^{n-1}R$$

Also ist nach dem Noetherschen Isomorphiesatz

$$I = \left\langle p^{n-i}(x_1^{s_i} - 1) + p^{n-1}w_i(x_1), p^{n-i}(x_2^{s_i} - 1) + p^{n-1}w_i(x_2) \mid 1 \leq i \leq n \right\rangle,$$

wobei $w_1(x_1) = 0$ und $\text{grad } w_i(x_1) < s_i$, $2 \leq i \leq n$, gewählt werden kann (analog für $w_i(x_2)$, $1 \leq i \leq n$).

Betrachte für beliebiges i , $2 \leq i \leq n$, das Polynom

$$p^{n-i}((x_1x_2)^{s_i} - 1) + p^{n-1}w_i(x_1x_2) - p^{n-i}(x_1^{s_i} - 1) -$$

$$- p^{n-1}w_i(x_1) - x_1^{s_i}(p^{n-i}(x_2^{s_i} - 1) + p^{n-1}w_i(x_2)) =$$

$$= p^{n-1}(w_i(x_1x_2) - w_i(x_1) - x_1^{s_i}w_i(x_2))$$

aus dem Ideal $I_{x_1} + I_{x_2}$.

Das Polynom $p^{n-1}(x_1^{s_i} - 1)$ ist aus I_{x_1} . Daher ist auch

$$p^{n-1}(w_i(x_1x_2) - w_i(x_1) - w_i(x_2))$$

aus $I_{x_1} + I_{x_2}$.

Da jedoch $\text{grad } w_i(x) < s_i$, $2 \leq i \leq n$, ist, folgt daraus, daß $w_i(x)$, $2 \leq i \leq n$, das Nullpolynom sein muß.

Wie in Satz 3 teilt jedes Polynom $x_1^{s_i} - 1$, $1 \leq i \leq n$, das vorhergehende Polynom $x_1^{s_i} - 1$.

Deshalb gilt für $1 \leq i \leq j \leq n$:

$$s_i \mid s_j$$

Die Übertragung dieses Ergebnisses auf den Gruppenring erfolgt wie in Satz 3'.

//

Mit diesem Satz hat man die Möglichkeit, jedes Ideal I mit der Eigenschaft E' aus dem Gruppenring $\mathbb{Z}\langle x_1, x_2 \rangle$ zu beschreiben.

Satz 11: Wenn ein Ideal I aus dem Gruppenring $\mathbb{Z}\langle x_1, x_2 \rangle$ die Eigenschaft E' hat, dann gibt es eine natürliche Zahl n mit der eindeutigen Primzahlzerlegung

$$n = \prod_{i=1}^r p_i^{n_i}$$

und Polynome $x_1^s - 1$ und $x_2^s - 1$, die folgende Darstellung von I liefern:

$$I = \left\langle n(x_1^s - 1), p_i^{n_i - j} (x_1^{s_{i,j}} - 1), \right. \\ \left. n(x_2^s - 1), p_i^{n_i - j} (x_2^{s_{i,j}} - 1) \mid 1 \leq i \leq r, 1 \leq j \leq n_i \right\rangle$$

Für s und $s_{i,j}$ gilt:

$$s \mid s_{i,j} \quad \text{für } 1 \leq i \leq r, 1 \leq j \leq n_i \\ s_{i,j} \mid s_{i,j+1} \quad \text{für } 1 \leq i \leq r, 1 \leq j \leq n_i - 1$$

Der Beweis dieses Satzes verläuft analog dem von Satz 4:

//

Mit Satz 11 hat man die Möglichkeit, bei beliebigen Wörtern $w(y,x)$, $y \in N$, $x \in G$, in einer Gruppe G zu entscheiden, ob für sie die Aussage von (B) wahr ist.

Umgekehrt liefert jedes Polynom aus einem in Satz 11 beschriebenen Ideal I in einer Gruppe G ein Wort $w(y,x)$, $y \in N$, $x \in G$, für das die Verallgemeinerung (B) von [1, Lemma 7] wahr ist.

Beispiel: Betrachte das Polynom

$$P(x) = 12(x^3 - 1) + 2(x^3 - 1)x^2 + (x^6 - 1)(x + 1) + \\ + (x^9 - 1)(x^2 - 1).$$

Es ist in einem Ideal I der in Satz 11 geforderten Gestalt enthalten.

Das entsprechende Wort hat die Form

$$w(y,x) = y^{P(x)} = y^{12(x^3-1)} y^{2(x^3-1)x^2} y^{(x^6-1)(x+1)} y^{(x^9-1)(x^2-1)} \\ = [x^3, y^{-12}] [x^3, y^2] x^2 [x, [y^{-1}, x^6]] [x^2, [y^{-1}, x^9]].$$

Literaturverzeichnis:

- [1] Hall, P. Some sufficient conditions for a
 group to be nilpotent.
 Illinois J. Math., vol. 2 (1958),
 pp. 787 - 801
- [2] Lambek, J. Lectures on Rings and Modules.
 Blaisdell Publishing Company
 Waltham, Mass. 1966
- [3] Neumann, H. Varieties of Groups.
 Springer Verlag, Berlin 1967
- [4] Schenkman, E. Group Theory.
 van Nostrand Company
 Princeton, New Jersey 1965
- [5] Specht, W. Gruppentheorie.
 Springer Verlag, Berlin 1956
- [6] Stroud, P. W. On a property of verbal and marginal
 subgroups.
 Proc. Camb. Phil. Soc., vol. 61 (1965),
 pp. 41 - 48

Lebenslauf

- 1943 geboren am 11. 10. als Sohn der Notarseheleute
Dr. Anton Nowak und Hanna Nowak, geb. Gerst,
in Rumburg/CSSR.
- 1949 - 1953 Besuch der Volksschule in Dettelbach am Main.
- 1953 - 1962 Besuch der Oberrealschulen in Scheinfeld und
Kitzingen.
- 1962 Abitur an der Oberrealschule in Scheinfeld.
- 1962 - 1969 Studium der Mathematik an den Universitäten
Würzburg, Wien und Erlangen-Nürnberg.
Vorlesungen bei den Professoren H. Bauer, E. Hlawka,
N. Hofreiter, G. Nöbeling und W. Specht.
- 1966 Vordiplom in Mathematik.
- 1969 Diplom in Mathematik
- 1969 - 1972 Tätigkeit als akad. Tutor und seit August 1972
als Verwalter einer Assistentenstelle am
Mathematischen Institut in Erlangen.

Offsetdruck-Fotodruck

J. Hogn, 8520 Erlangen, Hauptstr. 109 (Nähe Martin-Luther-Platz) Tel.22990
